Zum Bedarf nach Datenzugangsrechten

Früh, Alfred

Jusletter IT

Zum Bedarf nach Datenzugangsrechten

Autor/Autorin: Alfred Früh
Kategorie: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz, Wettbewerbsrecht
Zitiervorschlag: Alfred Früh, Zum Bedarf nach Datenzugangsrechten, in: Jusletter IT Flash 11. Dezember 2017

Die faktische Kontrolle eines Dateninhabers über bestimmte Daten kann sich negativ auf Dritte auswirken. Aus Sicht dieser Dritten – seien es einzelne Personen, betroffene Unternehmen oder gar die Gesellschaft als Ganzes – drängt sich deshalb die Frage auf, ob sie unter gewissen Voraussetzungen einen rechtlichen Anspruch auf Zugang zu faktisch geschützten Daten haben sollten. Der Beitrag zeigt auf, wann es zu Problemen kommt und skizziert in der Form neuer Datenzugangsrechte erste Lösungsansätze für diese Probleme.

Inhaltsverzeichnis

Alfred Früh
Dr.

Zum Bedarf nach Datenzugangsrechten

I. Ausgangspunkt

[1] Die Zuordnung (oder Nicht-Zuordnung) von Daten zu einem Rechtsträger (also einer natürlichen oder juristischen Person) ist relevant für alle Transaktionen, die Daten zum Gegenstand haben. Entsprechend ist sie auch zentral für die Datenwirtschaft, welche in hohem Masse auf die freie Verfügbarkeit und Handelbarkeit von Daten angewiesen ist. Vor diesem Hintergrund hat sich beispielsweise die Europäische Kommission zum Ziel gesetzt, einen möglichst freien Datenfluss (*free flow of data*) zu ermöglichen.[1] Eine besondere Komplexität erreicht die Thematik im Bereich der Personendaten, wo die Zuordnung von Daten zusätzlich eine Reihe anderer Fragestellungen, namentlich jene der informationellen Selbstbestimmung oder der Datenautonomie berührt.[2]

[2] Die Zuordnung von Daten zu einem Rechtsträger kann prinzipiell auf zwei Arten erfolgen: entweder rechtlich oder faktisch. Im Rahmen eines einjährigen Forschungsprojekts ist das Center for Information Technology, Society and Law (ITSL) zum Schluss gekommen, dass gegenwärtig die Einführung einer *rechtlichen* Zuordnung von Daten (im Sinne eines sog. Dateneigentums) nicht wünschenswert ist.[3] Dies gilt jedenfalls solange diese Zuordnung umfassend (und nicht bereichsspezifisch) erfolgen würde. Denn gleichzeitig wurde festgestellt, dass punktuell durchaus Handlungsbedarf besteht und bestimmte Probleme in der Praxis spezifisch gelöst werden sollten – was typischerweise ebenfalls mit Zuordnungsregeln geschieht.[4]

[3] Über die *faktische* Zuordnung von Daten ist damit aber noch nichts gesagt. Die Unternehmen der Datenwirtschaft sammeln, speichern und verarbeiten Daten prinzipiell in proprietären Silos, was ohne die Gewährung eines rechtlichen Schutzes solcher Daten auch kaum überrascht. In diesen Silos sind die Daten dem Zugang Dritter entzogen. Nicht nur aus Sicht des angestrebten *free flow of data* drängt sich die Frage auf, ob es nicht auch Konstellationen gibt, in welchen Dritten von Rechts wegen ein Zugang zu solchen faktisch kontrollierten Daten gewährt werden müsste.[5] Die wissenschaftliche Aufarbeitung dieser Frage steht indes noch am Anfang. Der Beitrag bietet einen schematischen Überblick über mögliche Datenzugangsrechte und erste Ansatzpunkte zu deren Ausgestaltung.

II. Systematisierung möglicher Datenzugangsrechte

[4] Zunächst kann zwischen dem Zugang zu eigenen Daten und dem Zugang zu Daten Dritter unterschieden werden.[6] Beim Zugang zu den eigenen Daten geht es konkret darum, ob der Inhaber der faktischen Kontrolle über Daten einen Rechtsanspruch auf Zugang zu diesen Daten haben sollte, wenn er die Kontrolle über diese Daten verloren hat (sogl. hinten 1). Beim Zugang zu Daten Dritter sind sodann mindestens zwei Varianten zu unterscheiden. Entweder wird der Zugang aus Gründen des öffentlichen Interesses ersucht (hinten 2) oder die Zugang

begehrende Partei braucht die Daten, um auf einem bestimmten Markt tätig zu sein (hinten 3).

[5] Mit Blick auf alle drei Varianten lauten die offensichtlichen Fragen: «Warum könnte sich ein solches Zugangsrecht rechtfertigen?» und: «Wie müsste bzw. könnte es ausgestaltet werden?». Beide Fragen sollen im Folgenden für alle drei Varianten kurz angerissen werden.

1. Zugang zu eigenen Daten

[6] Ein Dateninhaber, der die faktische Kontrolle über diese Daten verloren hat, bleibt unter Umständen ohne Rechtsbehelf – und zwar selbst dann, wenn er die Inhaberschaft unverschuldet verloren hat.[7] Allerdings stehen dem Inhaber bereits unter der gegenwärtigen Rechtslage mehrere Rechtsbehelfe zur Verfügung: Handelt es sich um Personendaten und liegt eine Datensammlung vor, kann er sich beispielsweise auf das datenschutzrechtliche Auskunftsrecht von Art. 8 DSG stützen.[8] Wenn Dritte die Daten des Inhabers speichern, dürfte typischerweise ohnehin ein Vertrag vorliegen. Zwingend ist dies allerdings nicht. Denkbar ist auch ein vertragsloser, z.B. auf einer Gefälligkeit beruhender Vertrag. Ebenfalls denkbar ist, dass der Vertrag kein Zugangsrecht vorsieht oder der Diensteanbieter ein Zugangsrecht gar vertraglich gültig abbedungen hat – wobei einem solchen Vorgehen durch die AGB-Kontrolle Grenzen gesetzt sind. Schliesslich bietet grundsätzlich auch das Deliktsrecht dem Inhaber die Möglichkeit, Zugang zu den Daten zur erhalten. Allerdings müsste dafür zum einen auch für Daten ein Realersatz deliktsrechtlich akzeptiert sein.[9] Zum anderen kann der deliktische Anspruch am fehlenden Verschulden oder – gar noch häufiger – an der fehlenden Widerrechtlichkeit scheitern: Absolute Rechte sind aufgrund des fehlenden urheber- und leistungsschutzrechtlichen Schutzes und des Fehlens eines *sui generis*-Schutzes für Datenbanken[10] eben gerade nicht verletzt und die einschlägigen objektiven Rechtsnormen des StGB vermögen ebenfalls nicht alle Fälle abzudecken. Entweder setzen sie eine besondere Sicherung der Daten voraus oder sanktionieren nicht das Vorenthalten des Zugriffs, sondern bloss die Beschädigung der Daten.[11]

[7] Im Wesentlichen bleiben damit drei typische Konstellationen, in denen der Inhaber ohne Rechtsbehelf bleibt: (1) Der Inhaber hat Daten ohne vertragliche Vereinbarung bei einem Dritten gespeichert und der Dritte enthält ihm den Zugriff vor. (2) Der Inhaber verliert einen Datenträger und die Daten sind bei Wiedererlangung des Datenträgers auf diesem nicht mehr vorhanden oder nicht mehr lesbar. (3) Der Inhaber verliert den Zugriff über Datenbestände, die er nicht besonders gesichert hat. Ob der fehlende Rechtsschutz in diesen Konstellationen tatsächlich ein neues Zugangsrecht rechtfertigt, bleibt näher zu untersuchen. Dabei stellt sich insbesondere die Frage, ob ein solches Recht nur konkret die genannten Fälle adressieren müsste oder umfassend ausgestaltet werden sollte. Gerade im zweiten Fall muss sorgfältig geprüft werden, ob es nicht zu unerwünschten Folgeproblemen kommen würde.[12]

[8] Erste Überlegungen zur Ausgestaltung eines solchen Zugangsrechts gehen dahin, dass es sich dem Besitzesrecht nachbilden liesse.[13] Wie die Instrumente des Besitzesrechts müsste

das Zugangsrecht nämlich auf die rasche Wiederherstellung der tatsächlichen Herrschaft gerichtet sein – allerdings mit dem Unterschied, dass der Adressat des Zugangsbegehrens seine Herrschaft über die Daten nicht verlieren würde.[14]

2. Zugang zu Daten Dritter im öffentlichen Interesse

[9] Die Nutzung grosser Datenmengen liegt nicht nur im Interesse der Daten sammelnden Unternehmen. Sie hat auch eine gesellschaftliche Dimension, weil sich damit fundamentale gesellschaftliche Probleme in ganz neuer Weise angehen lassen.[15] Vor diesem Hintergrund drängt sich die Frage auf, ob von Seiten der Öffentlichkeit nicht unter bestimmten Voraussetzungen ein Anspruch bestehen sollte, Zugang zu privat kontrollierten und der Öffentlichkeit *a priori* vorenthaltenen Daten zu erhalten. Drei Argumente können dafür ins Feld geführt und mit Beispielen unterlegt werden:

- Erstens kann ganz grundsätzlich argumentiert werden, Datennutzungen im öffentlichen Interesse dürften nicht dadurch unterbleiben, dass Unternehmen Daten in privaten Silos aufbewahren und nur selbst nutzen. Im Jahr 2008 begann Google, die Ausbreitung des Influenza- und Dengue-Virus anhand der weltweiten Suchanfragen zu modellieren.[16] Die Vorteile dieses Ansatzes sind offensichtlich: Es ist denkbar, beinahe in Echtzeit Informationen über den Ausbruch und die Verbreitung einer Pandemie zu erhalten. Zwar wurde das Programm – auch aufgrund unzutreffender Prognosen – inzwischen eingestellt.[17] Sollten solche Methoden aber in Zukunft mehr Erfolg haben (wovon auszugehen ist), wird es entscheidend sein, ob die Öffentlichkeit oder staatliche Stellen Zugang zu diesen Informationen haben. Ähnliche Beispiele zeigen, dass mit den anonymisierten Daten von Mobilfunkteilnehmern die Verbreitung von Bilharziose oder Malaria verfolgt werden kann.[18] Ebenfalls zu nennen ist die Nutzung von Randdaten bei der Strafverfolgung.[19]
- Zweitens könnte sich ein Zugangsrecht betreffend bestimmte Daten Privater besonders dann rechtfertigen, wenn die privaten Daten sich auf Infrastrukturen beziehen, die von der öffentlichen Hand zur Verfügung gestellt werden. Typische Beispiele sind Daten über die Nutzung von Strassen (mittels Positionsdaten der Mobiltelefone der Verkehrsteilnehmer)[20] oder Daten über die Nutzung des Elektrizitätsnetzes. Dieses Phänomen kann als *reverse public sector information (reverse PSI)* bezeichnet werden; die Information wird zwar nicht vom öffentlichen Sektor produziert, sollte diesem aber zugutekommen, weil sie sich auf dessen Infrastrukturen bezieht.[21]
- Drittens verbessern mehr Daten die Entscheidungsgrundlage der Behörden. So können Daten über Spitäler und Versicherungen die Kosten im Gesundheitswesen senken.[22] Geodaten, beispielsweise über Wasserpegel, Bodenbeschaffenheit oder Gesteinsbewegungen helfen den Behörden bei der Gefahrenanalyse[23], Daten über Emissionen erleichtern die Einhaltung von Umweltschutzzielen[24] und Unternehmensdaten erleichtern es, die richtigen Massnahmen zur Wirtschaftsförderung[25] zu treffen.

[10] Auch wenn es damit gute Gründe für ein solches Zugangsrecht gibt, steht man beim «Wie?» noch ganz am Anfang. Noch lässt sich nicht sagen, ob es eine übergreifende oder eine

punktuelle Lösung braucht. Zudem kann man sich auch fragen, wie der Anspruchsberechtigte überhaupt von der Existenz der Daten weiss. Dass das Zugangsrecht durch eine Art Zwangslizenz gewährt werden würde, ist zwar klar, die Krux steckt aber in der Formulierung der entsprechenden Voraussetzungen. Generell müssten die Eingriffsvoraussetzungen die Interessen der betroffenen Unternehmen berücksichtigen und dabei insbesondere den Geschäftsgeheimnissen Rechnung tragen.[26] Die Parameter der Zwangslizenz sind ebenfalls alle noch festzulegen, namentlich der Lizenzgegenstand («Welche Daten sind erfasst?»), die Weiterverwendung («Wozu dürfen die Daten überhaupt verwendet werden?») und die Lizenzgebühr («Handelt es sich um eine Gratislizenz oder ist ein Nutzungsentgelt geschuldet?»). Und schliesslich wäre auch noch zu klären, wer denn überhaupt anspruchsberechtigt sein soll.

3. Zugang zu Daten von Wettbewerbern

[11] Etwas anders präsentiert sich die Lage, wenn Unternehmen Zugang zu Daten anderer Unternehmen begehren, um auf einem bestimmten Markt wirtschaftlich tätig sein zu können. Oft dürfte es gar nicht um den Zugang zu demjenigen Markt gehen, auf dem der Adressat des Zugangsbegehrens bereits tätig ist, sondern vielmehr um den Zugang zu vor- oder nachgelagerten Märkten. Typisch ist etwa die Konstellation, dass ein Unternehmen auf einem nachgelagerten Markt Serviceleistungen erbringen will, wofür es auf bestimmte Daten aus dem vorgelagerten Markt angewiesen ist. Die Automobilindustrie ist beispielsweise eine jener Branchen, die solche mehrstufigen Liefer- und Leistungsketten kennt.[27]

[12] Die beschriebene Problematik ist aber nicht neu. Aus kartellrechtlicher Perspektive wird sie seit jeher im Rahmen der Missbrauchskontrolle unter der Fallgruppe der Liefer- oder Lizenzverweigerung behandelt, wobei in der Vergangenheit immer wieder das Schlagwort der *essential facility* verwendet wurde; zunächst im Zusammenhang mit unentbehrlichen Infrastruktureinrichtungen wie Brücken und Hafenanlagen[28], später bezogen auf Immaterialgüterrechte[29]. So gesehen dürfte es nur eine Frage der Zeit sein, bis auch in Bezug auf Daten wieder von *essential facilities* die Rede sein wird.

[13] Das Kartellrecht tut sich indes aus verschiedenen Gründen (und wie schon in Bezug auf Immaterialgüterrechte)[30] schwer damit, auf einfache Weise Zugang zu solchen wichtigen Daten zu gewähren. Die Verfahren dauern zu lange und sind zu umständlich. Letzteres ist auch der Tatsache geschuldet, dass die Abgrenzung kartellrechtlich relevanter Märkte (noch) unzureichend mit der Tatsache umgehen kann, dass viele Daten unentgeltlich zur Verfügung gestellt werden[31] und dass es sich oft um zwei- oder mehrseitige Märkte handelt, deren Interdependenzen mit den klassischen Instrumenten der Marktabgrenzung kaum überzeugend abgebildet werden können.[32] Auf das Kartellrecht in seiner gegenwärtigen Form ist damit kaum Verlass, wenn es darum geht, solche Zugangsprobleme zu lösen.[33]

[14] Damit gelangt man auch hier zur Frage, wie denn ein solches Zugangsrecht auszusehen hätte. Angesichts bereits bestehender sektorspezifischer Regeln, wie beispielsweise in der

Automobilindustrie[34] oder bei Bezahlsystemen[35], mag man zur Haltung neigen, eine sektorspezifische Regelung sei ausreichend. Andererseits gibt es keine Anzeichen dafür, dass sich das Problem nur in bestimmten Sektoren stellt. Daten sind heute in den meisten Branchen relevante Inputgüter, weshalb ein übergreifendes Zugangsrecht nicht von vornherein verworfen werden sollte.

[15] Auch dieses Zugangsrecht hätte die Form einer Zwangslizenz. Was den Stand der Forschung betreffend deren Ausgestaltung angeht, kann auf die vorstehenden Ausführungen verwiesen werden.[36] Allerdings drängen sich drei Präzisierungen auf: Erstens macht ein neues Instrument nur Sinn, wenn es nicht die Eingriffsvoraussetzungen des Kartellrechts (insbeondere ein via Marktabgrenzung und Marktanteilsberechnung ermitteltes Marktmachtkriterium) übernimmt. Zweitens spielt der Schutz von Geschäftsgeheimnissen hier eine noch grössere Rolle. Und drittens leuchtet unschwer ein, dass eine Zwangslizenz wohl nur entgeltlich eingeräumt werden dürfte, um die Innovations- und Investitionsanreize der Unternehmen nicht zu gefährden. Naheliegend wäre es, auf eine Lizenzierung zu FRAND-Bedingungen[37] zu setzen.[38]

III. Ausblick

[16] Auch wenn es noch vertiefter Forschung bedarf, um sachgerechte Instrumente zu entwerfen, lassen sich drei Punkte festhalten:

- Wenn es um die Zuordnung von Daten zu einem Rechtsträger geht, wird sich der Schwerpunkt der juristischen Forschung aller Voraussicht nach künftig von der rechtlichen Zuordnung (und damit vom sog. Dateneigentum) hin zur faktischen Zuordnung verschieben.[39] Damit rücken Datenzugangsrechte in den Vordergrund.
- Eine Systematisierung möglicher Datenzugangsrechte zeigt, dass mindestens drei verschiedene Konstellationen zu unterscheiden sind, für die jeweils unterschiedliche Rechtfertigungen vorgebracht werden können. Alle drei Fälle verlangen nach spezifischen Eingriffsvoraussetzungen, deren Konturen heute erst im Ansatz zu erkennen sind.
- Zwischen diesen drei Konstellationen gibt es aber auch Gemeinsamkeiten, oder besser: gemeinsame Schwierigkeiten. Eine davon ist, den Gegenstand exakt zu erfassen. Es wird beispielsweise nicht reichen, «Daten» herauszuverlangen, ohne dass geklärt ist, ob damit die syntaktische, semantische oder pragmatische Ebene angesprochen ist[40] und ob es sich um Rohdaten oder veredelte Daten handelt. Eine andere ist die Frage, ob die Zugangsrechte auf (sektor-)spezifische Probleme zugeschnitten werden sollen, deren Existenz empirisch nachgewiesen ist, oder ob sie so ausgestaltet werden sollen, dass sie prinzipiell unabhängig vom Verwendungskontext der Daten gelten – und so auch bislang unbekannte Probleme erfassen.

Dr. Alfred Früh, RA, ist Geschäftsführer des Center for Information Technology, Society, and

Law (ITSL) an der Universität Zürich und Co-Geschäftsführer des Schweizer Forum für Kommunikationsrecht (SF-FS).

---

1 Europäische Kommission, Communication from the Commission on Building a European Data Economy vom 10. Januar 2017, 5 ff.

2 S. Europäische Kommission (Fn. 1), 5, wonach sich daraus ein Spannungsverhältnis zum angestrebten *free flow of information* ergeben kann.

3 S. Florent Thouvenin/Rolf H. Weber, Zum Bedarf nach einem Dateneigentum, in: Jusletter IT Flash 11. Dezember 2017, Rz. 10 ff.

4 S. die Beiträge von Peter Georg Picht, Demian Stauber, Clara-Ann Gordon, Gregor Bühler, Peter K. Neuenschwander/Simon Oeschger und Lennart Chrobak, ebenfalls in diesem Jusletter IT Flash vom 11. Dezember 2017.

5 S. hierzu auch die Einsichten aus dem vom ITSL organisierten und vom Schweizerischen Nationalfonds (SNF) finanzierten internationalen Expertenworkshop, der vom 6. bis zum 8. Juli 2017 in Schaffhausen stattfand, abgedruckt im Workshop Summary (http://www.itsl.uzh.ch/dam/jcr:1a3604c6-04b0-47ef-92a8-a329edf191ee/Workshop%20Summary.pdf [alle Internetseiten zuletzt abgerufen am 1. Dezember 2017]), 2.

6 Der Beitrag baut hier und an weiteren Stellen auf Vorarbeiten von Rolf H. Weber und Florent Thouvenin auf, s. Rolf H. Weber/Florent Thouvenin, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018, erscheint demnächst.

7 Weber/Thouvenin (Fn. 6), D.II.

8 Michael Widmer, Rechte der Datensubjekte, in: Nicolas Passadelis/David Rosenthal/Hanspeter Thür (Hrsg.), Datenschutzrecht – Beraten in Privatwirtschaft und öffentlicher Verwaltung, Basel 2015, N 5.24.

9 Dies wurde in der schweizerischen Lehre und Rechtsprechung soweit ersichtlich bisher nicht thematisiert. Anders in Deutschland, s. die Hinweise bei Weber/Thouvenin (Fn. 6), D.II., Fn. 88.

10 Statt vieler Florent Thouvenin/Rolf H. Weber/Alfred Früh, Data ownership: Taking stock and mapping the issues, in: Matthias Dehmer/Frank Emmert-Streib (Hrsg.), Frontiers in Data Science, Boca Raton 2018, 126 ff.

11 Weber/Thouvenin (Fn. 6), D.II.

12 Weber/Thouvenin (Fn. 6), D.II.

13 Weber/Thouvenin (Fn. 6), D.II.

14 Weber/Thouvenin (Fn. 6), D.II.

15 Vgl. OECD, Data-Driven Innovation, Big Data for Growth and Well-Being, 2015, 197 ff.; Josef Drexl, Designing Competitive Markets for Industrial Data, Max Planck Institute for Innovation & Competition Research Paper No. 16–13, 62.

16 Paul Hofheinz/David Osimo, Lisbon Council Policy Brief, Making Europe a Data Economy: A New Framework for Free Movement of Data in the Digital Age, 2017, 8.

17 S. https://www.google.org/flutrends/about/.

18 S. das Data for Development (D4D)-Programm des Mobilfunkanbieters Orange (http://www.d4d.orange.com/en/presentation/endowment-and-panel/Folder/The-D4D-Challenge-is-a-great-success); Hofheinz/Osimo (Fn. 16), 8.

19 Weber/Thouvenin (Fn. 6), D.I.; Hofheinz/Osimo (Fn. 16), 17.

20 Hofheinz/Osimo (Fn. 16), 17; Europäische Kommission (Fn. 1), 12.

21 S. a. Max-Planck-Institut für Innovation und Wettbewerb, Position Statement of 26 April 2017 on the European Commission's «Public consultation on Building the European Data Economy», Rz. 28.

22 European Commission, Commission Staff Working Document on the Free Flow of Data and Emerging

Issues of the European Data Economy, vom 10. Januar 2017, 32; Weber/Thouvenin (Fn. 6), D.III.

23 European Commission (Fn. 22), 32

24 European Commission (Fn. 22), 32; Hofheinz/Osimo (Fn. 16),17.

25 Europäische Kommission (Fn. 1), 12.

26 Andreas Wiebe, Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäische Datenwirtschaft, CR 2017, 92, verweist hierbei auf Regelungen zum Schutz von Geschäftsgeheimnissen in der Richtlinie über die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Richtlinie).

27 Weber/Thouvenin (Fn. 6), D.I.; weitere Beispiele bei Max-Planck-Institut für Innovation und Wettbewerb, Data Ownership and Access to Data, Position Statement of 16 August 2016 on the Current European Debate, Rz. 9 f.

28 Grundlegend: *United States v. Terminal Railroad Association*, 224 U.S. 383 (1912).

29 S. z.B. Milan Jovanovic, Die kartellrechtlich unzulässige Lizenzverweigerung: Immaterialgüter als Essential-Facilities: Tatbestandsmerkmale und Rechtsfolgen, Diss. Zürich 2007.

30 Alfred Früh, Immaterialgüterrechte und der relevante Markt, Köln 2012, 452 ff., sowie zur *essential facilities*-Doktrin 399 ff.

31 S. dazu das deutsche Bundeskartellamt, das gestützt auf diese Tatsache eine Änderung des GWB fordert, Bundeskartellamt, Arbeitspapier «Marktmacht von Plattformen und Netzwerken», Ergebnisse und Handlungsempfehlungen, Juni 2016, 5; Bundeskartellamt, Competition Law and Data, May 2016, 27.

32 Thorsten Körber, Konzeptionelle Erfassung digitaler Plattformen und adäquate Regulierungsstrategien, ZUM 2017, 94; Bundeskartellamt, Competition Law (Fn. 31), 27; Daniel Schiess/Olivier Schaller, Herausforderungen im Wettbewerbsrecht, in: Florent Thouvenin/Rolf H. Weber (Hrsg.), Werbung – Online, Zürich 2017, 126 f.

33 S.a. Max-Planck-Institut für Innovation und Wettbewerb, (Fn. 27), Rz. 32 ff.; Drexl (Fn. 15), 67.

34 Zugang zu Reparatur- und Wartungsinformationen aufgrund der Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge, ABl. 2007 L 171/1.

35 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt – Zweite Zahlungsdiensterichtlinie (Payment Services Directive 2 – PSD 2), ABl. 2015 L 337/35. Die Richtlinie erlaubt Drittanbietern Zugang zu Kontoinformationen, s. auch Peter Lutz, Regulatorische Herausforderung von Bezahlsystemen: PayPal & Co, ZVglRWiss 2017, 185.

36 S. II.2 vorn.

37 FRAND steht für Fair, Reasonable And Non-Discriminatory.

38 Ebenso: Europäische Kommission (Fn. 1), 16; Weber/Thouvenin (Fn. 6), D.III.

39 So auch Max-Planck-Institut für Innovation und Wettbewerb (Fn. 21), Rz. 20 ff.

40 Zur Unterscheidung Herbert Zech, Information als Schutzgegenstand, Tübingen 2012, 51 ff.; Thouvenin/ Weber/Früh (Fn. 10), 120 f.

0 Kommentare

Es gibt noch keine Kommentare

** Pflichtfelder*

Was ist Ihr Kommentar?

Titel:

Ihr Kommentar: *

Name: *

Authorisierter Benutzer

Senden

Ihr Kommentar wird durch eine Moderatorin bzw. einen Moderator geprüft und in Kürze freigeschaltet.